

Exhibit ‘B’

DIGITAL FORENSICS CORP

Phase I Evaluation Report

Case Number	157307
Examiner Name	223

Received	
Completed	8/22/2018

TABLE OF CONTENTS

CLIENT DIRECTIVES.....	3
BACKGROUND.....	3
FORENSIC SCOPE OF WORK.....	4
PHASE I SCOPE OF WORK.....	4
PHASE II SCOPE OF WORK.....	4
CYBER HARASSMENT DOCUMENTATION	7
ATTEMPTED PHONE HACKING	7
IDENTITY THEFT AND MISAPPROPRIATION.....	8
SUSPICIOUS LINKEDIN ACCOUNT “GARY MORIN”	11
ONLINE HARASSMENT	12
WEB INVESTIGATION	13
INFO ABOUT MELODY JOY BROWN CANTU	13
TRACKING URLs.....	16
TRACKING URL RESULTS	20
ENGINEER’S SUMMARY AND RECOMMENDATIONS	23
CONCLUSION.....	24
APPENDIX A – SAMPLE POLICE REPORT	25

CLIENT DIRECTIVES

DR. SANDRA GUERRA (the "Client") has requested the following:

1. Conduct a digital investigation on a known suspect; and
2. Discover the identity of an unknown cyber-harasser.

BACKGROUND

By the work of an unknown person, the Client has been the victim of:

1. **Attempted Phone Hacking:** attempted intrusion into Client's mobile phone account via Client's mobile phone service provider;
2. **Identity Theft and Misappropriation:** the creation of accounts on dating websites using Client's email address; and
3. **Defamation:** Untrue statements concerning the Client which harms the Client.

In addition to the above, the Client has also been the victim of harassment caused by **MELODY JOY BROWN CANTU** when the Client's social network received unwanted messages disparaging the Client's character from Ms. Cantu.

Cyber harassment - also known as cyber bullying or internet harassment --refers to the malicious use of technology to willfully and deliberately HARASS, HARM, or DEFAME another individual or entity.

FORENSIC SCOPE OF WORK

PHASE I SCOPE OF WORK

1. The scope of work for a Phase I Evaluation of a cyber harassment digital forensics case is to record and document the online harassment, harm, or defamation.
2. Phase I includes the collection, extraction, recovery, and preservation of all data from available client devices and online accounts and performing an extensive search of the online presence of the suspects based on the information provided.
3. Phase I also includes the creation of tracking URLs to target at the suspect(s). The client will send the tracking URLs to the suspect(s) and Digital Forensics Corporation (DFC) will monitor the tracking URLs for any activity by the suspect(s).

PHASE II SCOPE OF WORK

1. A Phase II Examination for cyber harassment is primarily an external action phase for a digital forensics investigation which may include initiating a legal proceeding for the purposes of issuing a subpoena against any third-party entities (such as internet service providers (ISPs), phone service providers (PSPs), or online service providers (OSPs)) to discover the suspects' true identities.
2. Phase II includes the creation of a searchable archive of all data successfully collected, extracted, recovered, and preserved, from all devices and/or accounts, as part of Phase I.

3. A Phase II Examination will also include the all information discovered by DFC's exhaustive web investigation of the suspect(s) based on the results of the Phase I Evaluation.
4. If the client is interested in proceeding to Phase II, the client needs to file a police report at the local police station to document the cyber harassment or cyber fraud. The client should attach the entire "Phase I Evaluation Report" to the police report as documentation of the cyber harassment or cyber fraud.
 - a. If, prior to the conclusion of the Phase I investigation, the client has already filed a police report with the client's local jurisdiction, the client should "supplement" the existing police report by including a copy of this "Phase I Evaluation Report".
5. In Phase II, the client will need to provide the following to Digital Forensics Corporation (DFC):
 - Copy of filed and time-stamped police report (which has been supplemented with DFC's Phase I Evaluation Report).
6. In Phase II, Digital Forensics Corporation (DFC) will provide any IP addresses obtained as a result of DFC's tracking URLs engineered specifically for the client. If a suspect clicks on a DFC tracking URL, the IP address of the individual will be relayed to DFC. With additional legal work, the IP address can be used to determine the physical location and/or identity of the suspect.
7. In Phase II, Digital Forensics Corporation will coordinate with and support an outside attorney who will file the official legal pleadings and discovery requests in order to obtain any information associated with the suspects which may be retained by third-parties (such as ISPs, PSPs, or OSPs). The filed police report (containing the Phase I

Evaluation Report), results of DFC's tracking URL campaign, and any additional information provided by the client such as an affidavit will be used for the official legal

Many internet service, phone service, and online service providers have very specific requirements regarding the release of their clients' personal information; therefore, it is very important to structure and submit a formal request in the correct and proper form according to all the requirements.

inquiry.

- a. Please note that in an official legal inquiry such as a complaint to discover the identity of a cyber harasser, a party (such as an ISP or social media website) may decline or object to a legal request for information about the identity of account owners and/or subscribers. In that case, DFC will continue supporting and coordinating with the outside attorney to provide a response to the objection or file another subpoena to obtain relevant information regarding the identity of the individual of interest. The client understands that this process may involve additional costs to account for additional subpoenas being served. DFC services will only cover supporting an outside attorney for serving the additional subpoena; however, DFC cannot represent the client in court. DFC is not a lawfirm and will not represent you in any legal capacity. If authorized, we will attempt to locate a licensed attorney to represent you and that engagement will be between you and the attorney and governed by the terms of an engagement agreement. The engagement letter will state that you agree that DFC may be engaged in a consulting capacity with the attorney(s) and any compensation will be governed by DFC's agreement with the attorney assigned to your case.
8. Although DFC cannot guarantee any particular outcome, the intent of a Phase II investigation is to assist the client in preparation for legal action against the actual person(s) responsible for the cyber harassment or cyber fraud.

CYBER HARASSMENT DOCUMENTATION

Digital Forensics Corporation performed investigation and documentation of attempted phone hacking, identity theft and misappropriation, and defamation. DFC engineers acquired all evidence related to the acts described above. This evidence is documented below.

ATTEMPTED PHONE HACKING

An unknown malicious hacker attempted to gain access to Client’s Verizon mobile phone account (account number 521731356-00001) (the “Verizon Account”). The Client’s account came under attack at the following times:

Date	Time
May 16, 2018	1:15 PM
May 18, 2018	12:32 AM
May 18, 2018	11:46 AM
May 20, 2018	9:32 AM
May 24, 2018	2:42 PM
May 31, 2018	4:22 PM
June 2, 2018	10:20 PM
June 6, 2018	11:07 AM

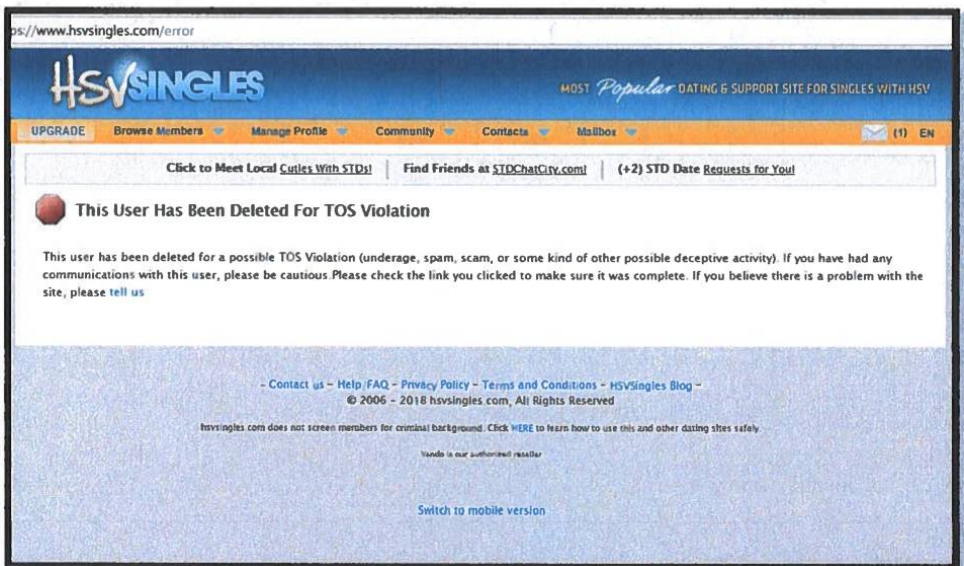
On June 8, 2018, at 1:15 AM, Verizon notified Client that the Verizon Account would have its online account access removed due to an excessive and suspicious number of failed log-in attempts on the Verizon Account’s voicemail. As a result, the Client could only restore voicemail access by agreeing to remove online account access.

IDENTITY THEFT AND MISAPPROPRIATION

The Client's email address (drsandragera@yahoo.com) was used by an unknown individual to create profiles on two social media websites dedicated to people with sexually transmitted diseases. These accounts were both created with the nickname "MonkeyBar1970".

Client contacted the websites and asked them to suspect and/or remove the accounts. One of the websites, positivesingles.com at 416-682-1072 via Lisa John, informed Client that the account MonkeyBar1970 was set up with Client's email from IP **72.179.171.30** at 4:26 PM on Tuesday, May 22, 2018, from an iPhone. This IP address is located somewhere in the greater San Antonio area. No other information about who created MonkeyBar1970 was available.


Evidence showing "MonkeyBar1970" existed but has since been removed.



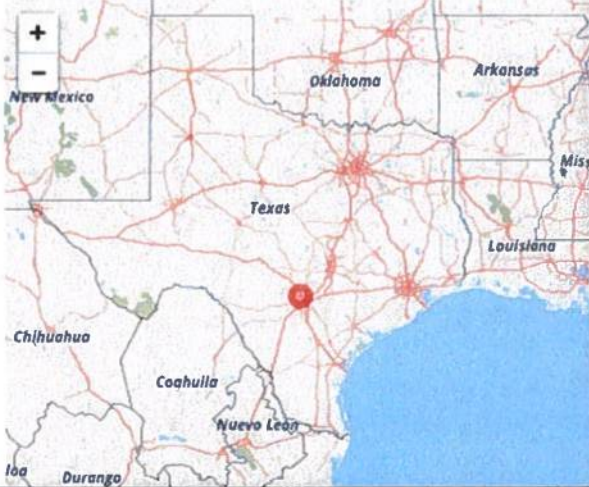
IP Address from which the MonkeyBar1970 account was created is located in San Antonio.

[Lookup IP Address](#)

Details for 72.179.171.30

IP: 72.179.171.30
Decimal: 1219734302
Hostname: 072-179-171-030.res.spectrum.com
ASN: 11427
ISP: Spectrum
Organization: Spectrum
Services: None detected
Type: [Broadband](#)
Assignment: [Dynamic IP](#)
Blacklist: [Click to Check Blacklist Status](#)
Continent: North America
Country: United States 
State/Region: Texas
City: San Antonio
Latitude: 29.5698 (29° 34' 11.28" N)
Longitude: -98.6161 (98° 36' 57.96" W)
Postal Code: 78249

Geolocation Map



Positivesingles.com is a Florida-based website and subject to the laws of Florida.

Showing results for: positivesingles.com

Original Query: positivesingles.com

Contact Information

Registrant Contact

Name: Moniker Privacy Services

Organization: Moniker Privacy Services

Mailing Address: 2320 NE 9th St,
Second Floor, Fort Lauderdale FL
33304 US

Phone: +1.8006886311

Ext:

Fax: +1.9545859186

Fax Ext:

Email:

e810aa3c058043b11429de6b1564
87930525dcad480cb1fa6c42408f2
9fbf1e8@positivesingles.com whoi
sproxy.org

Admin Contact

Name: Moniker Privacy Services

Organization: Moniker Privacy Services

Mailing Address: 2320 NE 9th St,
Second Floor, Fort Lauderdale FL
33304 US

Phone: +1.8006886311

Ext:

Fax: +1.9545859186

Fax Ext:

Email:

e810aa3c058043b11429de6b1564
87930525dcad480cb1fa6c42408f2
9fbf1e8@positivesingles.com whoi
sproxy.org

Tech Contact

Name: Moniker Privacy Services

Organization: Moniker Privacy Services

Mailing Address: 2320 NE 9th St,
Second Floor, Fort Lauderdale FL
33304 US

Phone: +1.8006886311

Ext:

Fax: +1.9545859186

Fax Ext:

Email:

e810aa3c058043b11429de6b1564
87930525dcad480cb1fa6c42408f2
9fbf1e8@positivesingles.com whoi
sproxy.org

On August 21, 2018, DFC contacted the second website, hvsingles.com, was contacted at 888-494-2850 via customer service agent "Rose". HSVSingles said they could not reveal the IP address from which the account MonkeyBar1970 was created, but would do so upon receipt of a copy of a police report filed in this matter. They requested the time-stamped police report be faxed to them at 866-599-9719 (ATTN: Donna).

HSVsingles.com is a Florida-based website and subject to the laws of Florida.

Showing results for: hsvsingles.com

Original Query: hsvsingles.com

Contact Information

Registrant Contact

Name: Dating Media Group
Organization: Dating Media Group
Mailing Address: 6919 W
BROWARD BLVD, STE 270,
Plantation FL 33317 US
Phone: +18007702715
Ext:
Fax:
Fax Ext:
Email: helpdesk@dmgbill.com

Admin Contact

Name: Dating Media Group
Organization: Dating Media Group
Mailing Address: 6919 W
BROWARD BLVD, STE 270,
Plantation FL 33317 US
Phone: +18007702715
Ext:
Fax:
Fax Ext:
Email: helpdesk@dmgbill.com

Tech Contact

Name: Dating Media Group
Organization: Dating Media Group
Mailing Address: 6919 W
BROWARD BLVD, STE 270,
Plantation FL 33317 US
Phone: +18007702715
Ext:
Fax:
Fax Ext:
Email: helpdesk@dmgbill.com

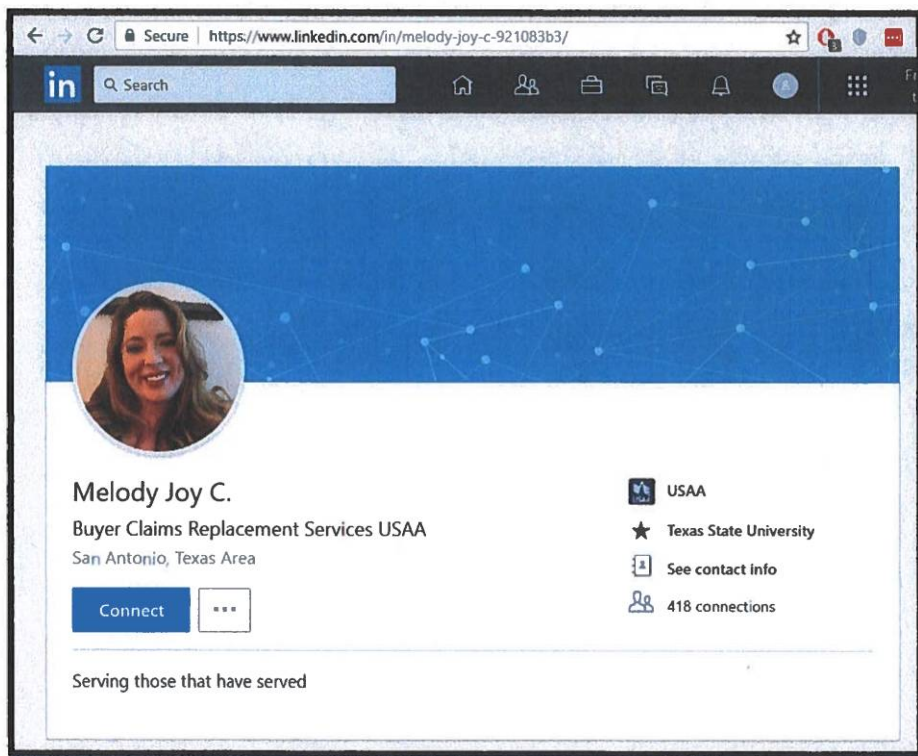
SUSPICIOUS LINKEDIN ACCOUNT "GARY MORIN"

DFC Engineers acquired and archived the Client's LinkedIn and Facebook accounts. The LinkedIn user "Gary Morin" contacted Client. Gary Morin is believed to be a fake account. Gary Morin has sent a request for adding to Sandra Guerra's friends of LinkedIn.

- **"Gary Morin to Sandra Guerra, "5/22/18, 1:46 AM" INCOMING"**

ONLINE HARASSMENT

The Client's social media contacts were harassed and the Client defamed by the online Facebook username "Joy Brown" and LinkedIn username "Melody Joy Cantu". On May 20, 2018, Melody Joy Cantu contacted Nate Bellinger, the Client's friend, on LinkedIn. Mr. Bellinger has no knowledge of Joy Brown, online or offline. On May 20, 2018, Joy Brown contacted Mr. Bellinger's ex-wife, Stacey Bellinger, through Facebook. Ms. Bellinger also had no prior knowledge of Joy Brown, online or offline. Client believes Joy Brown and Melody Joy Cantu are usernames of Melody Joy Brown Cantu, Client's ex-husband's current wife.



WEB INVESTIGATION

Forensic Examiner conducted Web Investigation to identify additional information regarding individuals responsible or suspected of harassment.

INFO ABOUT MELODY JOY BROWN CANTU

Our engineers performed a thorough web-search using advanced tools and techniques. As the result of the reconnaissance phase, the following information about investigated person was found:

result for Melody Cantu...

7 profiles found 0 photos found 0 relatives found 1 phone #'s found 40 websites found 1 usernames found 1 emails found

1 LOCATION(S) FOUND

SAN ANTONIO, TX

Plaza De Armas

San Fernando Cathedral

Main Plaza

Dolorosa

Drury Plaza Hotel San Antonio Riverwalk

The Esquire Tavern

SP Parking

The Westin Riverwalk, San Antonio

Map data ©2018 Google

0 RELATIVE(S) FOUND

1 PHONE NUMBER(S) FOUND

+1 210-425-5765

1 EMAIL(S)

joyandtyrus@hotmail.c...

7 PROFILE(S)

Facebook Joy Cantu

Pinterest Joy Cantu


Instagram Joy Brown

Youtube Joyandtyrus

Ebay Tyrusandmolly

Etsy Tyrusandmolly

Deviantart Viridianeye


1 SOURCE:  Facebook

URL: <https://www.facebook.com/joy.brown.7967>

IDENTIFIERS: [Possible Match](#) [Joy Cantu](#) [Joybrown.7967](#)

IP: 31.13.76.70

SCORE: Exact



Timeline About Friends Photos More

DO YOU KNOW JOY?

To see what she shares with friends, send her a friend request.

Photos

Friends

Joy Cantu updated her cover photo.
July 24 at 7:58 PM

Finally Together!

Comprehensive Report

Comprehensive Report

Date: 08/21/2018

Reference ID: NONE

Report Legend

D - Deceased Person

Relatives

S > - 1st Degree of Separation
S >> - 2nd Degree of Separation
S >>> - 3rd Degree of Separation

Subject Information

(Best Information for Subject)

Name: **MELODY JOY CANTU** (05/30/2014 to 06/04/2018)Name: **MELODY JOY ROSS** (06/01/2003 to 04/25/2018)Name: **MELODY JOY BROWN** (12/01/1994 to 04/01/2017)Name: **JOY BROWN** (09/01/2001 to 07/12/2016)Name: **JOY ROSS** (07/02/2004 to 11/02/2013)Name: **MELODY JOY BEAN** (07/01/1999 to 02/01/2009)Date of Birth: **01/20/1976**, Born 42 years agoOther Names Associated with Subject
None foundOther DOBs Associated with Subject
None found

Possible Phones Associated with Subject:

(210) 425-5765 (CT) (Mobile) (86%)
 (210) 290-9734 (CT) (ActiveLandLine) (78%)
 (210) 277-0817 (CT) (LandLine) (66%)
 (210) 392-5275 (CT) (Mobile) (66%)
 (210) 641-9811 (CT) (LandLine) (66%)
 (210) 688-0656 (CT) (66%)
 (512) 733-1619 (CT) (66%)
 (512) 864-9533 (CT) (66%)
 (608) 278-1319 (CT) (LandLine) (66%)

Indicators

Bankruptcies: No

Liens: No

Judgments: No

Properties: Yes

Corporate Affiliations: No

Criminal/Traffic: No

Global Watch Lists Match: Yes

Email Addresses Associated with Subject

joyandtyrus@hotmail.comfrancene16@hotmail.comaross2@sabx.rr.com

FORENSIC EXAMINATION DISCLOSURE: Forensic Examiner searched for information using a variety of third-party resources. As a result, data contained in this report might include false positives, and might require further verification.

TRACKING URLs

Our forensic examiners have created some links that will help us identify people, but we need your cooperation.

- Tracking URLs are links which send back information to the link creator when the link is clicked by a device on the internet.
- Each individual tracking URL captures IP address, operating system, browser, screen resolution, and hash information for the device from which the tracking URL is clicked. This information can be used in court proceedings to determine the identity of anonymous or unknown online individuals.
- In this case, the Forensic Examiner created unique tracking URLs for the client to send or target at the suspects.
- **FIRST:** Please click the following links, which will provide us with your IP address so we can exclude it from the results (to prevent false-positives in case you accidentally click on any of the others).
 - **NOTE:** Click on **ONE** link per device (so if you have 2 phones and a laptop, click on a separate link for each device). If you need additional links, let us know.

Cx_Sandra_Guerra:

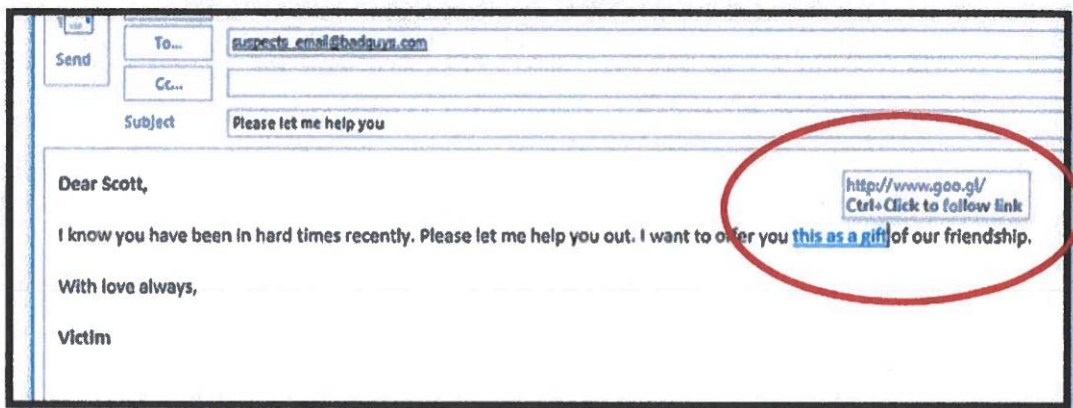
<https://goo.gl/J5GE9Z>

- **NEXT:** Our forensic examiner created the following tracking URLs the suspect(s). They are designed to help us identify suspects in your case. You need to send the URL to each suspect on whatever platform (email, social media, text message) works best for that suspect.

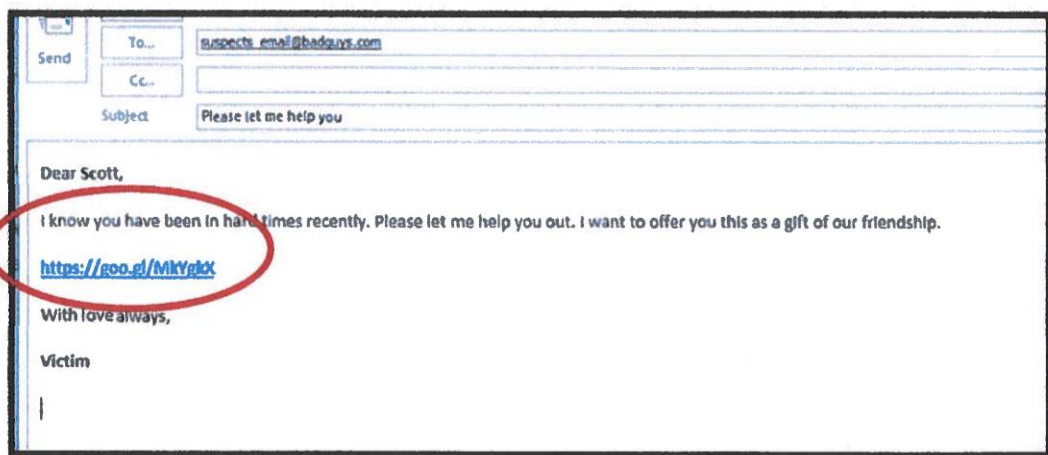
*** * * DO NOT CLICK ON THESE LINKS YOURSELF * * ***

- You need to include the link in a message containing something the suspect might be interested enough to click on: **DO NOT MENTION THE REAL PURPOSE BEHIND THE LINK.** The message could be something like “I’d like to send you money,” or “You will not believe this,” **along with that URL created for that suspect.** Be creative, but do not reveal what the link really is.
- Ideally, a separate tracking URL should be sent to each and every device and/or account from/to which the harassment has occurred or is occurring.
- The tracking URLs can be sent either as embedded hyperlinked text (see (i) below) or as a stand-alone link separate from the text (see (ii) below). We suggest sending the tracking URL using method (i), an embedded hyperlink, if possible.

(i): An example of sending a tracking URL as a link embedded in the text.



(ii): An example of sending a tracking URL as a stand-alone link.



- Once a tracking URL link is accessed, DFC will receive a report with the detected IP address and location from which tracking URL access is detected, which then will be used to identify the Internet Service Provider (ISP) and the approximate location of the suspect.

- Below are the unique tracking URLs created for this case:

Client-directed tracking URLs

Melody_Cantu: <https://goo.gl/QLpCG>

Rodrigo_Cantu: <https://goo.gl/yMEEVj>

DFC-directed tracking URLs

Melody_Joy_From_Teresa: <https://goo.gl/9gqCA1>

Dr.Cantu_From_Melissa: <https://goo.gl/7fifqF>

Melody_Joy_via_Phone: <https://goo.gl/sCbWZZ>

If additional tracking URLs are needed, more can be created.

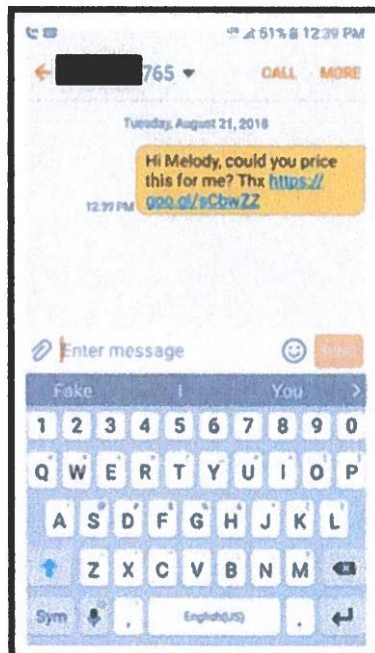
IMPORTANT NOTE:

- Client is advised to notify DFC immediately after sending tracking URLs to the missing individual. DFC examiners will immediately start IP address tracking.
- If the client accidentally clicks on a tracking URL, the client should immediately notify DFC to avoid false positives.
- If additional tracking URLs be needed, the client should let DFC know and more tracking URLs will be provided.
- Any information obtained, including IP addresses, will be extracted, analyzed, and provided to the client in a Phase II report.

TRACKING URL RESULTS

- In the Phase I Process, the DFC Forensic Examiner created specific Tracking URLs to send to the individuals performing the alleged harassing.
- Tracking URLs were sent to the appropriate communication platform for the suspects to click on. When activated tracking URLs capture recipient's geographic location (city) and IP address. IP address can provide approximate location.
- Once a tracking URL link is accessed, the DFC will receive a report with the detected IP address and location from which tracking URL access is detected, which then will be used to identify the Internet Service Provider (ISP).

Sample DFC-created tracking URLs targeted at suspect.



- Below are the preliminary results and IP Information of the tracking URLs activated to date:

Tracking Link: "Melody_Joy_via_Phone" <https://goo.gl/sCbwZZ>


First Click	2018-08-21 12:42:08
IP Address	72.179.164.76
User OS	Mac OS X
User Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_1) AppleWebKit/601.2.4 (KHTML, like Gecko) Version/9.0.1 Safari/601.2.4 facebookexternalhit/1.1 Facebot Twitterbot/1.0
Device	Safari
Second Click	2018-08-21 12:42:14
IP Address	72.179.164.76
User OS	iPhone
User Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_1) AppleWebKit/601.2.4 (KHTML, like Gecko) Version/9.0.1 Safari/601.2.4 facebookexternalhit/1.1 Facebot Twitterbot/1.0 Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_1) AppleWebKit/601.2.4 (KHTML, like Gecko) Version/9.0.1 Safari/601.2.4 facebookexternalhit/1.1 Facebot Twitterbot/1.0
Device	Safari

Device and OS Information – Device and OS information can be important circumstantial and/or corroborating evidence when attempting to discover the true identity of an unknown or anonymous harasser.


The IP discovered as a result of this tracking link is located in San Antonio.

[Lookup IP Address](#)

Details for 72.179.164.76

IP: 72.179.164.76
Decimal: 1219732556
Hostname: 072-179-164-076.res.spectrum.com
ASN: 11427
ISP: Spectrum
Organization: Spectrum
Services: None detected
Type: [Broadband](#)
Assignment: [Dynamic IP](#)
Blacklist: [Click to Check Blacklist Status](#)
Continent: North America
Country: United States 
State/Region: Texas
City: San Antonio
Latitude: 29.5698 (29° 34' 11.28" N)
Longitude: -98.6161 (98° 36' 57.96" W)
Postal Code: 78249

Geolocation Map



ENGINEER'S SUMMARY AND RECOMMENDATIONS

- Based on the evidence provided to Digital Forensics Corporation by Client and Digital Forensics Corporation's independent investigation, **we conclude that a Phase II Forensics Examination is recommended.**

- Phase I Evaluation Report is intended for internal communication between client and Digital Forensics Corporation; and informs the client about relevance of findings. Phase I is not intended for use in courtrooms, presentation to opposing counsel, arbitration, and any other legal proceedings.
- Phase II Full Examination Report is admissible in court, and includes a notarized Affidavit of the authenticity of digital evidence.

CONCLUSION

PHASE II FORENSIC EXAMINATION – Phase II is intended to discover the identity of the perpetrator(s) and/or suspect(s), as well as eliminate potential persons of interest. The results of the tracking URLs, which report back to Digital Forensics Corporation the IP address of the device when and if the URL is clicked, will be used in the process of discovering the true identity of the suspect(s). If these efforts are unsuccessful in discovering the true identity of the suspect, DFC will assist the client in resorting to legal action to compel the relevant parties (internet service provider, phone service provider, and online service provider) to produce evidence related to the suspect.

The client is advised to:

- **File a police report with the appropriate police department and attach a copy of this Phase I Evaluation Report to it (or add it as a “supplement” if a police report already exists);**
- **Provide a time-stamped copy of the police report, containing this Phase I Evaluation Report, to DFC;**
- **Send out DFC’s tracking URLs to the suspect(s) and click on the tracking URL for the client him/herself; and**
- **Alert DFC of any ongoing cyber harassment.**

Although Digital Forensics Corporation uses the best available forensic practices and technologies, DFC cannot guarantee any particular outcome or that any specific information will be discovered during a forensic examination.

APPENDIX A – SAMPLE POLICE REPORT

Case Number: _____
 Date: _____
 Reporting Officer: _____
 Prepared By: _____

Incident Type: Cyber Harassment.
 Attempted Phone Hacking;
 Identity Theft and Misappropriation;
 Defamation;

Victim(s): Dr. Sandra Guerra

Address: _____

Evidence: Digital Forensics Corporation's *Phase I Evaluation Report*
 (attached hereto as **Exhibit A**)

I, Dr. Sandra Guerra, am a victim of cyber harassment, attempted phone hacking, identity theft and misappropriation, and defamation.

First beginning on or about May 16, 2018, , I began to be cyber harassed. The harassment included attempted phone hacking, identity theft and misappropriation, and defamation, among other things. This harassment was conducted by an UNKNOWN person(s). This harassment is documented in the Phase I Evaluation Report attached hereto as **Exhibit A**. As a result of this harassment, I have been HARMED personally and professionally.

I have hired a digital forensics company, Digital Forensics Corporation, to conduct an independent investigation. They are currently working on identifying the individual(s) responsible for this cyber harassment and assisted me with documentation of cyber harassment as indicated in the report attached hereto as **Exhibit A**.

I am interested in identifying and pursuing legal action against the individual or individuals responsible for this harassment against myself, my friends, and my family.

Name: _____

Date: _____